IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application Of: Lee Ming Cheng, et al.	§	Attorney Docket No. P-370.240
Serial No.: 10/074,124	§	Group Art Unit: 2131
Filed: February 12, 2002	§	Examiner: Chai Longbit

Title: SEQUENCE GENERATOR AND METHOD OF GENERATING A PSEUDO RANDOM SEQUENCE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION UNDER 37 CFR 1.132 FROM DR LEE MING CHENG

I, Lee Ming Cheng, hereby declare that:

1. I am a co-inventor in the above application and am familiar with the application and pending claims.

2. I am an Associate Professor of the Department of Electronic Engineering, City University of Hong Kong, China. I received a PhD from the University of London 1982. My areas of expertise and research interests include Security Encoding, Card Technology, Security Technology and Encryption. I have been awarded over US$ 3.5M in grant funding in the past 6 years for research in these areas. I have published 43 journal papers, 3 book chapters, 65 research conference papers and filed 11 patent applications. I am a Fellow of the IEE and a Senior Member of the IEEE

3. Claims 1 through 10 of the above patent application are rejected by the United States Patent and Trademark Office as allegedly unpatentable. Claims 7 through 10 are rejected as allegedly unpatentable over Beker (Patent No. 4,748,576) in view of Roth (Patent No. 5,243,650) and claims 1 through 6 are rejected as allegedly unpatentable over Beker in view of Roth and in view of Puhl

(Patent No. 5,365,585). I have reviewed each of the three US patents used in rejecting the claims of the above patent application and based on my knowledge and expertise in this field, it is my opinion that the combination of the three cited US patents does not teach every feature of the presently claimed invention, nor can the method or devices disclosed in the three cited patents be properly combined as suggested by the Examiner.

4. In part 6 of the Office Action dated January 27, 2006 the Examiner's position is that Becker Figure 1 teaches all of the elements of claim 7 except how to generate each bit of the second plurality of binary sequences, but that Roth teaches this in Figure 5. Claim 7 requires:

in the linear feedback shift registers, generating a first plurality of binary sequences,

in the nonlinear function generators, applying a plurality of nonlinear functions to said the first plurality of binary sequences to obtain an uncorrelated second plurality of binary sequences, and

randomly selecting an output sequence from one of the second plurality of binary sequences.

Roth, in Figure 5, teaches a non-linear function having a plurality of linear feedback shift registers at its input. The nonlinear function is constructed by using a feedback path connecting the function output as a delayed input.

Beker teaches a plurality of logic gates to construct two linear feedback shift registers (LFSR T) and (LSFR S). LFSR T is the Data Input to a multiplexer that selects the binary sequence to a PRBS output. The multiplexer is controlled by LFSR S at its Address Input. There is a close temporal (timing) relationship between the Data Input B0B1...B32; i.e. B0=T0(t); B1=T1(t)=T0(t-1)....;B32=T32(t)=T0(t-31). This strongly correlated relationship restricts the randomness of the output. By incorporating the non-linear function taught by Roth between one or both LSFRs and the multiplexer Address and/or Data inputs, they become totally separated from each other. Randomization would be difficult to maintain in such a device because the LSFRs information fed into the Address and Data Inputs is totally separated (orthogonal). The use of address line to control data output will not achieve the decorrelation requirements and thus the PRBS output is still strongly correlated with the data input. Thus, the combination would not work with the teachings of Beker and Roth.

The combination can only work from that date of our patent application because we teach that the same LSFR first sequences are fed into both function generators A and B and the same data in A is used to generate decorrelation properties and is fed to the controller of the multiplexer. We teach that a correlation behavior has to be known to the system before a decorrelation behavior can be

derived. Therefore, insufficient information is given in Beker and Roth to combine the teachings successfully in the way required by claim 7.

5. The Examiner rejects claim 8 because Beker allegedly teaches a one-to-many relationship between the first and second plurality of Binary sequences. Beker does not teach any relationship between the first and second plurality of Binary sequences because the examiner admits it does not teach the second plurality of binary sequences.

The multiplexer Data Input 31-to-1 of Beker have a strong relationship in time. We cannot call this a one-to-many relationship because by building a temperal table of the output, the sequence can easily be cipher-analyzed. A one-to-many relationship in cipher terms would be one where an input is mapped onto different outputs by a Boolean operation selected in the non linear function. This will destroy the temperal relationship of the output data because the output sequence is generated by a Boolean function on a plurality of input sequences which do not have any common repetitive patterns.

Therefore, Beker does not teach a one-to-many relationship as Beker's "many" is limited by a predefined estimated small size.

6. The examiner rejects claims 1 and 2 because it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teachings of Beker with the system of Roth and then further with the teachings of Puhl. As I have stated in paragraph 4 above Beker and Roth do not provide enough information to successfully combine their systems.

Besides, Beker teaches a plurality of logic gates to construct a linear feedback shift register to generate a plurality of binary sequence but it does not teach a plurality (two or more) of linear feedback shift registers to generate a plurality of binary sequences AND a controller. Beker teaches one linear feedback shift register (LFSR T) and one controller (LFSR S). Beker teaches a direct selection by a simple single multiplexer (switch). It does not teach *at least first and second switches.* There is no teaching in any of the documents to add a second switch and so the combination cannot teach *the first switch operative to select one of said second plurality of binary sequences to the first bit of the shift register, and the second switch operative to select one of said second plurality of binary sequences to an output.*

Beker does not expressly state the use of a feedback controller. Nothing in Beker shows to have any part of the PRBS output of the multiplexer fed back to the controller (LFSR S). Roth has feedback, but this is used to construct the non-linear function by using a feedback path

connecting the function output as a delayed input. It does not suggest a feedback controller. So, the prior art documents do not show *the first switch operative to select one of said second plurality of binary sequences to the first bit of the shift register* (controller).

Roth does not teach *at least first and second nonlinear function generators having said first plurality binary sequences as their input, the first nonlinear function generator operative to generate a second plurality of binary sequences and the second nonlinear function generator operative to generate a third plurality of binary sequences.* Roth teaches a single non-linear function having a plurality of linear feedback shift registers at its input. Because there is only one multiplexer in Beker only one Non linear function output would be contemplated. There is nothing in any of the prior art documents to tells us to add a second multiplexer.

7. I have studied the three prior art documents carefully and based on my knowledge and expertise in this field, nothing in those documents shows how to make the sequence generator and method claimed in our patent application. How to successfully combine the systems of Beker, Roth and Puhl only becomes apparent when they are further combined with the teachings of our patent application.

6. I hereby declare that all statements made herein of my own knowledge are true, that all statements made on information and belief are believed to be true, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Date: 26/06/2006

Lee Ming Cheng, Ph.D.